AMENDMENT TO THE CLAIMS

Please amend the claims to read as shown below. This listing of claims will replace all previous versions and listings of claims in the application.

1. (Currently Amended) A computer-implemented method for gathering security event data and rendering result data in a manageable format comprising the steps of:

a plurality of security devices generating security event data comprising a plurality of alerts ~~with a plurality of security devices at a first location~~ in response to detecting a security event in a distributed computing environment, the security devices being logically coupled to a computer having a display;

the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data as result data;

the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable ~~providing one or more variables operable for analyzing and filtering the security event data, the~~ variables comprising at least one of a location of a security event, a source of security event, and a destination address of the security event~~, a security event type, a priority of a security event, and an identification of a system that detected a security event~~;

~~creating scope criteria by selecting one or more of the variables operable for analyzing and filtering the security event data;~~

the computer collecting the security event data generated by the plurality of security devices ~~located at the first location~~;

the computer storing the collected security event data ~~at a second location~~;

~~analyzing and~~ the computer filtering the collected security event data using the one or more user-configurable variables ~~with the scope criteria~~ to produce the result data for the event data report;

the computer transmitting the result data to one or more clients; and

the one or more clients displaying the event data report comprising the result data ~~comprising filtered alerts based on the scope criteria~~.

2. - 3. (Canceled)

4. (Currently Amended) The method of Claim 1, wherein collecting the security event data comprises

a sensor generating security event data ~~from a sensor~~;

the sensor sending the security event data ~~from the sensor~~ to a collector coupled to the computer; and

the computer converting the event data to a common format.

5. (Canceled)

6. (Currently Amended) The method of Claim 1, further comprising the computer searching the stored security event data for additional information identifying a security event.

7. - 48. (Canceled)

49. (Currently Amended) A method for managing security event data collected from a plurality of security devices in a distributed computing environment comprising the steps of:

a plurality of security devices generating security event data ~~with a plurality of security devices~~ in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts;

the security devices sending the security event data to a computer coupled to a display;

the computer transferring the security event data for storage in a database;

the computer presenting a user interface via the display for configuring an event data report that identifies a portion of the security event data as result data;

the computer receiving a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable ~~applying a scope criteria comprising one or more definable variables to the security event data for analyzing and filtering the security event data to produce a result, the~~ variables comprising at least one of ~~a location of a security event, a source of security event, a destination address of the security event,~~ a security event type, a priority of a security event, and an identification of a system that detected a security event;

the computer filtering the stored security event data using the one or more user-configurable variables to produce the result data for the event data report;

~~accessing the result with one or more clients coupled to an application server;~~ and

. the computer displaying via the display the event data report and the result data comprising filtered alerts based on the user-configurable variables ~~scope criteria~~.

50. - 59. (Canceled)

60. (New) The method of Claim 1, further comprising the step of the security devices pre-filtering the security event data prior to transmitting the pre-filtered security event data to the computer.

61. (New) The method of Claim 1, further comprising the step of performing an analysis on the collected security event data, the analysis comprising at least one of (a) comparing a source address of a first detected security event with a source address of a second detected security event and (b) comparing information associated with each detected security event with information identifying a known vulnerability of the distributed computing environment.

62. (New) The method of Claim 49, further comprising the step of the security devices pre-filtering the security event data prior to transmitting the pre-filtered security event data to the computer.

63. (New) The method of Claim 49, further comprising further comprising the step of the computer searching the stored security event data for additional information identifying a security event.

64. (New) The method of Claim 49, further comprising the step of performing an analysis on the stored security event data, the analysis comprising at least one of (a) comparing a source address of a first detected security event with a source address of a second detected security event and (b) comparing information associated with each detected security event with information identifying a known vulnerability of the distributed computing environment.

65. (New) The method of Claim 49, further comprising the step of the computer converting the security event data into a common format.

66. (New) A computer program product for gathering security event data and rendering result data in a manageable format, the computer program product comprising:

a computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code comprising:

computer-readable program code to receive security event data from a plurality of security devices, the security event data comprising a plurality of alerts in response to detecting a security event in a distributed computing environment;

computer-readable program code to present a user interface via a display for configuring an event data report that identifies a portion of the security event data as result data;

computer-readable program code to receive a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a location of a security event, a source of security event, and a destination address of the security event;

computer-readable program code to store the received security event data;

computer-readable program code to filter the received security event data using the one or more user-configurable variables to produce the result data for the event data report; and

computer-readable program code to display the event data summary comprising the result data.

67. (New) The computer program product of Claim 66, further comprising computer-readable program code to convert the received security event data into a common format.

68. (New) The computer program product of Claim 66, further comprising computer-readable program code to search the received security event data for additional information identifying a security event.

69. (New) The computer program product of Claim 66, wherein the received security event data comprises data pre-filtered by at least one of the plurality of security devices.

70. (New) The computer program product of Claim 66, further comprising computer-readable program code to perform an analysis on the received security event data, the analysis comprising at least one of (a) comparing a source address of a first detected security event with a source address of a second detected security event and (b) comparing information associated with each detected security event with information identifying a known vulnerability of the distributed computing network.

71. (New) A computer program product for managing security event data collected from a plurality of security devices in a distributed computing environment, the computer program product comprising:

a computer-readable storage medium having computer-readable program code embodied therewith, the computer-readable program code comprising:

computer-readable program code to receive security event data from a plurality of security devices in response to detecting a security event in a distributed computing environment, the security event data comprising a plurality of alerts;

computer-readable program code to store the received security event data in a database;

computer-readable program code to present a user interface via a display for configuring an event data report that identifies a portion of the security event data as result data;

computer-readable program code to receive a selection via the user interface of one or more user-configurable variables operable for filtering the security event data, the user-configurable variables comprising at least one of a security event type, a priority of a security event, and an identification of a system that detected a security event;

computer-readable program code to filter the received security event data using the one or more user-configurable variables to produce the result data for the event data report; and

. computer-readable program code to display the event data report and the result data comprising filtered alerts based on the selected variables.

72. (New) The computer program product of Claim 71, further comprising computer-readable program code to convert the received security event data into a common format.

73. (New) The computer program product of Claim 71, further comprising computer-readable program code to search the received security event data for additional information identifying a security event.

74. (New) The computer program product of Claim 71, wherein the received security event data comprises data pre-filtered by at least one of the plurality of security devices.

75. (New) The computer program product of Claim 71, further comprising computer-readable program code to perform an analysis on the received security event data, the analysis comprising at least one of (a) comparing a source address of a first detected security event with a source address of a second detected security event and (b) comparing information associated with each detected security event with information identifying a known vulnerability of the distributed computing network.